REMARKS

INTRODUCTION

In accordance with the foregoing, no claims have been amended. Claims 33-35 have been cancelled. Claims 1-32 are pending and under consideration.

CLAIM REJECTIONS

Claims 1-3, 5-7, 11, 12 and 23-25 were rejected under 35 USC 102(e) as being anticipated by Kawan et al. (US 7,039,812) (hereinafter "Kawan").

Claims 24-26 and 33-35 were rejected under 35 USC 102(b) as being anticipated by Sime (US 5,386,104) (hereinafter "Sime").

Claims 4 and 13-15 were rejected under 35 USC 103(a) as being unpatentable over Kawan as applied to claims 3 and 11, and further in view of Saito et al. (US 6,980,672) (hereinafter "Saito").

Claims 8-10, 18-20, 31 and 32 were rejected under 35 USC 103(a) as being unpatentable over Kawan as applied to claims 1 and 24, and further in view of O'Connor et al. (US 6,938,159) (hereinafter "O'Connor").

Claims 16, 17, 21 and 22 were rejected under 35 USC 103(a) as being unpatentable over Kawan in view of Saito as applied to claim 15, and further in view of Sime.

Claims 27-30 were rejected under 35 USC 103(a) as being unpatentable over Sime as applied to claim 26, and further in view of Saito.

Kawan discusses a system and method for user authentication. In Kawan, requesting an additional shared secret, such as a PIN 44, or additional credentials, such as documentation 36, thus establishing multiple layers of authentication, augments the authentication method. Kawan, 4:26-4:30.

In addition to presentation and comparison of a biometric 26, such as a fingerprint 28, an aspect of an embodiment of the present invention involves the comparison of additional biometrics 26, such as the user's voice 30 or face 32, a document 36, or perhaps a PIN 44, in effect, combining biometrics 26 and PIN 44 or other information in a single process. When the user 10 comes to the system 14 and presents a biometric 26, such as the user's fingerprint 28, the way in which the user 10 presents the fingerprint 28 is unique to the particular user 10.

Further, only the particular user 10 knows the way he or she presents the fingerprint 28. Kawan, 4:40-4:51.

In Kawan, codes are used to open the smart card 66. The user 10 presents his or her fingerprint 28 to the smart card 66 and presents a PIN 44 to the smart card 66 and opens the smart card 66, and the smart card 66 has enough information to be secure. Assume that the user 10 has, for example, a digital signature or digital certificate 40 that was signed by someone else. The user 10 can use that particular digital signature 40 safely sitting on the user's smart card 66 to authenticate himself, but basically the user's smart card 66, to the host computer 18. Also, the user 10 can present his or her biometric information 26 with the user's PIN 44 to the host computer 18, and the smart card 66 is not needed. Thus, it is not necessary for the user 10 to have the smart card 66 or anything else, but simply to present himself or herself, and it becomes unnecessary to authenticate the smart card 66 and then solve some other problem to prove that it was signed by the proper authority and that the authority is trusted. Kawan, 8:19-8:37 and Figure 1.

Further in Kawan, the verification parameters of user credentials 24, such as threshold levels for matching of fingerprints 28, the quality of scanners, or the tolerance to input biometrics 26, such as the case of cuts on a user's finger, can be controlled by the authority, such as the host computer 18, in the user authentication process, depending on the risk of the application run by the authority 18 and the strength of the predefined shared secret 42. The strength of the secret 42 is controlled by the authority 18 and forces the user 10 to present the user's credentials 24 under the directions of the authority 18. For a lower level of security, this can be by presenting one or more fingerprints 28. For a higher level of security, it can be verification of fingerprints 28, voice 30, and iris 34 of the user 10 in the predefined sequence 46. At the same time, the authority 18 can adjust the threshold levels for each biometric template to a lower or higher level to allow a desired level of control of the secure access. Kawan, 9:47-9:64.

Sime discusses a system and method for detecting user fraud in automated teller machine transactions. In Sime, an ATM 10 includes a conventional user interface unit or fascia 14 incorporating key operated input means 16 for enabling a user of the ATM 10 to enter, if required, a personal identification number (PIN) and to select desired services provided by the ATM 10. Sime, 3:13-3:20 and Figures 1 and 2.

Further in Sime, in the memory unit 42 of the host computer 12 is a suspicion count 42. This is a count of the number of consecutive suspicious transactions performed by a user. A suspicious transaction is one in which output data from the biometric means 40 fails to match conclusively the reference biometric data for the relevant user but lies within a predetermined limit of discrepancy. Each time that a suspicious transaction takes place, the total of the suspicion count is incremented by one. On the other hand, when a non-suspicious transaction is completed by a user, the suspicion count is decremented to zero. A suspicion count threshold number, either for a particular user or for all users, may be determined and stored in the host computer 12, for example, in the user reference file 36. Sime, 4:42-4:56.

Still further in Sime, each ATM 10 also includes a transaction authorization module 44, which is a software module that is integrated into the processing means 32 which controls the operation of the ATM 10, the module 44 serving to authorize a transaction selected by a user. The inputs to the transaction authorization module 44 are as follows: the predicted transaction; the actual requested transaction; the biometric reference value; and any previously recorded suspicion count. The outputs from the transaction authorization module are: OK, meaning that the identity of the user has been confirmed and that the user can proceed with the transaction; failed, meaning that the biometric test has not confirmed the identity of the user as read from his identification card, thereby implying that an attempted fraud is taking place; and suspicious, meaning that the module 44 cannot be 100% sure either way. In the last instance, the suspicion count in the memory unit 42 is incremented by one, so that the system is aware of a possible attempted fraud. It should be understood that if the suspicion count reaches a predetermined threshold value (typically 3) then the module 44 terminates the transaction. Sime, 4:57-5:10.

Claims 1-10 and 23

Independent claim 1 recites: "...setting a first threshold value if the input password matches with a registered password and setting a second threshold value if the input password does not match with the registered password..." In contrast to claim 1, Kawan does not discuss setting threshold values based on if a correct password was entered. In Kawan, the verification parameters of user credentials 24, such as threshold levels for matching of fingerprints 28, the quality of scanners, or the tolerance to input biometrics 26, such as the case of cuts on a user's finger, are controlled by the authority depending on the risk of the application run by the authority 18 and the strength of the predefined shared secret 42. Note that the shared secret 42 is separate and different from the PIN 44 discussed in Kawan. The shared secret 42 is

established between the user 10 and the authority 18 and consists of a predefined sequence 46 of presenting the previously enrolled user's biometrics 26 and/or other predefined credentials 24, such as documentation 36 in the form of passports or certificates. The strength of the secret 42 is controlled by the authority 18 and forces the user 10 to present the user's credentials 24 under the directions of the authority 18. For a lower level of security, this can be by presenting one or more fingerprints 28. For a higher level of security, it can be verification of fingerprints 28, voice 30, and iris 34 of the user 10 in the predefined sequence 46. At the same time, the authority 18 can adjust the threshold levels for each biometric template to a lower or higher level to allow a desired level of control of the secure access. As such, Kawan discusses a system where thresholds are set in accordance to either the shared secret, or a predetermined threshold based on the sensitivity of the transaction a user wishes to perform. Kawan does not discuss setting the threshold based on a correct or incorrect password as is recited in claim 1.

Claims 2-10 and 23 depend on claim 1 and are therefore believed to be allowable for at least the foregoing reasons.

Withdrawal of the foregoing rejection is requested.

Claims 11-22

Independent claim 11 recites: "...a threshold value setting unit which sets a first threshold value if the input password matches with a registered password and sets a second threshold value if the input password does not match with the registered password..." In contrast to claim 11, Kawan does not discuss threshold value setting unit setting thresholds based on if a correct password was entered. In Kawan, the verification parameters of user credentials 24, such as threshold levels for matching of fingerprints 28, the quality of scanners, or the tolerance to input biometrics 26, such as the case of cuts on a user's finger, are controlled by the authority depending on the risk of the application run by the authority 18 and the strength of the predefined shared secret 42. Note that the shared secret 42 is separate and different from the PIN 44 discussed in Kawan. The shared secret 42 is established between the user 10 and the authority 18 and consists of a predefined sequence 46 of presenting the previously enrolled user's biometrics 26 and/or other predefined credentials 24, such as documentation 36 in the form of passports or certificates. The strength of the secret 42 is controlled by the authority 18 and forces the user 10 to present the user's credentials 24 under the directions of the authority 18. For a lower level of security, this can be by presenting one or more fingerprints 28. For a

higher level of security, it can be verification of fingerprints 28, voice 30, and iris 34 of the user 10 in the predefined sequence 46. At the same time, the authority 18 can adjust the threshold levels for each biometric template to a lower or higher level to allow a desired level of control of the secure access. As such, Kawan discusses a system where thresholds are set in accordance to either the shared secret, or a predetermined threshold based on the sensitivity of the transaction a user wishes to perform. Kawan does not discuss a threshold setting unit setting the threshold based on a correct or incorrect password as is recited in claim 11.

Claims 12-22 depend on claim 11 and are therefore believed to be allowable for at least the foregoing reasons.

Withdrawal of the foregoing rejection is requested.

Claims 24-32

Claim 24 recites: "...adjusting a threshold level of a biometrics device which reads a user's biometric information based on a password input by a user, wherein the threshold level is broadened when the user inputs a valid password to increase the possibility of the user being authenticated by the biometrics device, and the threshold level is narrowed when the user inputs an invalid password to decrease the possibility of the user being authenticated by the biometrics device." In contrast to claim 24, neither Kawan nor Sime discusses adjusting a threshold value of a biometric device based on if a valid password was entered. Regarding the rejection of claim 24 based on Kawan, in Kawan, the verification parameters of user credentials 24, such as threshold levels for matching of fingerprints 28, the quality of scanners, or the tolerance to input biometrics 26, such as the case of cuts on a user's finger, are controlled by the authority depending on the risk of the application run by the authority 18 and the strength of the predefined shared secret 42. Note that the shared secret 42 is separate and different from the PIN 44 discussed in Kawan. The shared secret 42 is established between the user 10 and the authority 18 and consists of a predefined sequence 46 of presenting the previously enrolled user's biometrics 26 and/or other predefined credentials 24, such as documentation 36 in the form of passports or certificates. The strength of the secret 42 is controlled by the authority 18 and forces the user 10 to present the user's credentials 24 under the directions of the authority 18. For a lower level of security, this can be by presenting one or more fingerprints 28. For a higher level of security, it can be verification of fingerprints 28, voice 30, and iris 34 of the user 10 in the predefined sequence 46. At the same time, the authority 18 can adjust the threshold

levels for each biometric template to a lower or higher level to allow a desired level of control of the secure access. As such, Kawan discusses a system where thresholds are set in accordance to either the shared secret, or a predetermined threshold based on the sensitivity of the transaction a user wishes to perform.

Regarding the rejection of claim 24 based on Sime, Sime does not discuss that the biometric reference values are adjusted for any reason as is recited in claim 24. Sime revolves around a suspicion count. If the suspicion count goes over a certain number, then the transaction is cancelled. However, the threshold values of biometric inputs is not altered based on thes suspicion counts as is recited in claim 24.

Claims 25-32 depend on claim 24 and are therefore believed to be allowable for at least the foregoing reasons.

Withdrawal of the foregoing rejection is requested.

Claims 33-35

Claims 33-35 have been cancelled.

CONCLUSION

There being no further outstanding objections or rejections, it is submitted that the application is in condition for allowance. An early action to that effect is courteously solicited.

Finally, if there are any formal matters remaining after this response, the Examiner is requested to telephone the undersigned to attend to these matters.

If there are any additional fees associated with filing of this Amendment, please charge the same to our Deposit Account No. 19-3935.

Respectfully submitted,
STAAS & HALSEY LLP

Date: June 19, 2006

By: Gregory W. Harper
Gregory W. Harper
Registration No. 55,248

1201 New York Avenue, NW, 7th Floor
Washington, D.C. 20005
Telephone: (202) 434-1500
Facsimile: (202) 434-1501